REMARKS

Claims 4, 6-7 and 24-29 are pending. Claims 4, 7 and 24 are the independent claims.

I. Office Action Summary

In the Office Action dated January 23, 2008, the Examiner rejected all of the claims as obvious over the combination of Hirota et al. (U.S. 6, 856,431 – "Hirota") and Dolan et al. (U.S. 5, 604,801 – "Dolan")

II. Rejections Under 35 U.S.C. § 103(a)

Applicants respectfully disagree with the Examiner's rejection the claims over Hirota et al. and Dolan et al.

CLAIM 4

Amended independent claim 4 recites:

A device for playback of encrypted audio and/or video files from a memory card, the device comprising:

a processor; and

a module operatively coupled with the processor and configured for:

obtaining an encrypted key from a protected area of the memory card;

retrieving a fractional portion of an audio and/or video file from the memory card;

decrypting the obtained encrypted key;

decrypting the fractional portion of the audio and/or video file with the decrypted key; and

deleting the decrypted key after decrypting the fractional portion of the audio and/or video file before decrypting an additional fractional portion of the file.

(emphasis added)

Hirota, as described in the prior response, and as admitted in the Office Action dated January 23, 2008 (page 8), is lacking at least the "deleting" step of claim 4. Applicants note that the citation on page 8 of the Office Action relating to the Hirota passage at col. 15, lines 45-53 does not disclose decrypting about two seconds of content a key before the key are deleted (page 8, last paragraph, Jan. 23, 2008 OA). Instead, the cited passage merely identifies AOB frames each having around 2 second of playback time. The cited passage does not state how many frames are decrypted at one time and does not even mention keys or decryption. Furthermore, at col. 42, lines 30-42 and col. 47, lines 21-27, Hirota recites the use of a single "FileKey" being used for the AOB frames in a given AOB file. As noted in the prior response, there is no teaching or suggestion in Hirota of deleting a key between decryption of fractional portions of a file.

Dolan fails to make up for the deficiencies in Hirota. Dolan discloses a communication system for public key data communications. Dolan is cited by the Examiner as allegedly disclosing the step of deleting the decrypted key before decrypting an additional fractional portion of the file. Applicant respectfully disagrees with this characterization of Dolan. Dolan discloses a communication system that uses a server, separate from a party sending a message, to perform public key processing on the message sent by a sending party, so that the sending party doesn't have to perform the public key processing on the sending party's portable security device (Col. 2, lines 54-64). The process disclosed in Dolan involves the message sending party sending a key encrypting key (KEYa), along with the message to be processed, to the server (FIG. 4a). The server then signs the message by decrypting a secret key (SKa) already stored on the server, signing the entire message using the secret key, and either forwarding

the message or returning it to the sending party to send on to the recipient (Col. 6, line 66 – Col. 7, line 11; FIG. 4b). The decrypted secret key at the server is temporarily stored, used to digitally sign the message from the sending party, and then erased (Col. 7, lines 2-11; FIG. 4b).

Dolan fails to teach or suggest any of the elements of claim 4, including the step the Office Action admits is missing from Hirota. Claim 4 recites "deleting the decrypted key . . . before decrypting an additional fraction." Dolan is related to a way of digitally signing communications in a communication system using standard public-private key encryption. Dolan is not related to a decryption process of items in a memory device. In essence, Dolan describes a form of outsourced ***encryption*** of ***entire*** messages in a communication system rather than decryption of fractional portions of the content of an encrypted file in a memory. Dolan is unrelated to memory devices, discusses encryption (digitally signing) of messages rather than decryption of data and discusses encryption for entire messages before deleting a key used to encrypt the message.

Accordingly, Applicants respectfully submit that claim 4 distinguishes over Dolan and Hirota, alone or in combination for at least the above reasons. Claims 6 and 35-38 are dependent claims, therefore their allowability directly follows from the allowability of independent claim 4.

CLAIM 7

Claim 7 relates to a computer readable storage medium having an executable program configured to:

> decrypt an encrypted audio or video file from the memory card,
>
> wherein decrypting the audio or video file comprises:
>
> (a) decrypting a key stored in the memory of the device;
>
> (b) **decrypting a portion of the audio or video file less than an entirety of the audio or video file**;
>
> (c) **deleting the decrypted key**; and

(d) **repeating (a) through (c) until the entirety of the audio or video file is decrypted.**

(emphasis added)

Claim 7 recites a computer readable medium with an executable program configured to, *inter alia,* delete a decrypted key after each portion of a file is decrypted, until the entire file is decrypted. Accordingly, for at least the same reasons as noted for claim 4, Applicants submit that claim 7 is allowable over the cited art.

III. New Claims 35-51

Applicants have added new claims 35-51 relating to the elected invention (identified by the Examiner as "playback of encrypted content by decrypting a factional portion of copied encrypted content . . ."). Applicants submit that claims 35-51 are fully supported by the specification as filed and that no new matter has been added. Claims 35-38 are dependent on claim 4. Claim 39 is a new independent claim and claims 40-51 depend from claim 39.

CLAIM 39

Claim 39 recites a method for playback of encrypted audio and/or video files stored on a memory, where the method includes:

> obtaining an encrypted key from a protected area of the memory card with a device having a processor and a memory operatively connected with the processor;
> retrieving a fractional portion of an audio and/or video file from the memory card with the device;
> decrypting the copied encrypted key;
> decrypting the fractional portion of the audio and/or video file with the decrypted key; and
> **deleting the decrypted key from the device after decrypting the fractional portion of the audio and/or video file before decrypting an additional fractional portion of the audio and/or video file.**

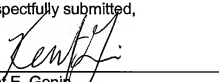
(emphasis added)

Although of different scope than claims 4 and 7, claim 39 recites steps relating to deleting a decrypted key after each portion of a track is decrypted and before the next fractional portion of the file is decrypted. Accordingly for at least the same reasons as noted for claims 4 and 7, Applicants submit that claim 39 is allowable over the cited art. Claims 40-51 are dependent claims. Accordingly, their allowability directly follows from the allowability of independent claim 39.

IV. Conclusion

Applicants amended claims 4 and 6-7 to broaden the claims while focusing on the novel and non-obvious features currently cited therein. The amendments and new claims 35-51, as described above, are fully supported by the specification, add no new matter, and fall within the elected invention identified by the Examiner. With the above remarks, Applicants submit that claims 4, 6-7 and 35-51 are in condition for allowance. A Notice of Allowance is respectfully requested.

Respectfully submitted,



BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200

Kent E. Genin
Registration No. 37,834
Attorney for Applicants